Why the DVD Hack Was a Cinch

by Andy Patrizio

2:15 p.m. 2.Nov.1999 PST

The anonymous developers of the decryption program that removes DVD copy protection had an easy time doing it, thanks to a gaffe by a software developer and the surprising weakness of the encryption technology.

Essentially, the two European hackers who developed the DeCSS utility that copies a DVD movie disc were able to break the code because one of the product's licensees inadvertently neglected to encrypt the decryption key.

Industry experts were stunned by the hack because DVD as a movie-playing format is supposed to be copy-proof. In fact, DVD would not be on the market today without the permission of the motion picture industry which, sources say, is reeling from this development.

Breaking DVD's encryption was considered extremely difficult, but once the first key was discovered, the rest fell with ease, since the crackers were able to use their original, valid key as a launch point to find more valid decryption keys.

DeCSS is a tiny (60 KB) utility that copies the encrypted DVD video file, which has a .VOB extension, and saves it to the hard disc without encryption.

Since DVD movies can range in size from 4.7 GB to 9.4 GB and recordable DVD has at best 2.5 capacity (or 5.2GB for double-sided discs), direct DVD copying is unfeasible. But starting next year, 4.7 GB recordable DVD drives will hit the market, making duplication of DVD discs much easier.

DVD uses a security method called the Content Scrambling System. CSS is a form of data encryption used to discourage reading media files directly from the disc without a decryption key. To descramble the video and audio, a 5-byte (40-bit) key is needed.

Why the DVD Hack Was a Cinch page 2

2:15 p.m. 2.Nov.1999 PST

continued

Every player -- including consoles from Sony, Toshiba, and other consumer electronics vendors, as well as software vendors for PCs like WinDVD and ATI DVD -- has its own unique unlock key. Every DVD disc, in turn, has 400 of these 5-byte keys stamped onto the disc. That way, the unlock key from every licensee, be it WinDVD or a Pioneer DV-525 unit, will read the disc.

All licensees of DVD technology have to encrypt their decryption key so no one can reverse-engineer the playback software and extract the key.

Well, one licensee didn't encrypt their key. The developers of DeCSS, a Norwegian group called MoRE (Masters of Reverse Engineering) got a key by reverse-engineering the XingDVD player, from Xing Technologies, a subsidiary of RealNetworks.

"We found that one of the companies had not encrypted their CSS decryption code, which made it very easy for us," said Jon Johansen, a founder of MoRE, in Norway. "We didn't think it would be that easy, in fact."

RealNetworks did not return repeated calls requesting comment.

Because the unlock key is 5 bytes long, Johansen and his two partners, who wish to remain anonymous, were able to guess a whole slew of other keys. So even if all future DVD movies remove the Xing key, DeCSS has a plethora of other keys to choose from.

Johansen and his partners were able to guess more than 170 working keys by trial and error before finally just giving up to go do something else. "I wonder how much they paid for someone to actually develop that weak algorithm," said Johansen. "It's a very weak encryption algorithm."

Leaving such a weak link in the security chain surprised industry people. "I am really surprised that they made it that easy to break into," said Kevin Hause, senior analyst with International Data Corp. "One of the key concerns about DVD was security."
"I don't think it's the end of the world, but it'll be interesting to see what steps the industry takes now, whether they start delaying the releases of certain titles," said Bill Hunt, webmaster of The Digital Bits, a DVD news site.
"I would expect it could also delay the advent of recordable DVD, because it'll give people a medium to write these hacked video files."
Others aren't so talkative. The Motion Picture Association of America (MPAA) declined to comment. The DVD Forum, based in Japan, was unreachable due to a national holiday, but it did issue a carefully worded statement.
"The circulation through the Internet of the illegal and inappropriate software is against the stream of copyright protection. Toshiba, which has led the establishment of the DVD format and is the chair-company of the DVD Forum, feels it is a great pity," wrote Masaki Mikura, manager of the strategic partnership and licensing division at Toshiba Ltd.
"In the future, the laboratories will be more actively conducting strict surveillance and take counter measures against illegal, inappropriate software and hardware in the market. Moreover, we believe that, based on the recent legislation, legal measures and steps will be taken by copyright holders against such violation of intellectual properties," Mikura wrote.

###